UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/887,585	06/21/2001	David W. Carman	NA01-00201	8239

28875 7590 07/19/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 07/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	Application No. 09/887,585	Applicant(s) CARMAN ET AL.	
	Examiner Benjamin E. Lanier	Art Unit 2132	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 07 July 2005 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____ months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1,3,5-19,21,23-39*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____
13. ☒ Other: Explanation of how amended claims would be rejected.

Gilberto Barron Jr.

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Continuation of 11. does NOT place the application in condition for allowance because: Applicant's argument that there is no motiviation to combine the teachings of Tatebayashi and Mizikovsky is not persuasive because Mizikovsky removes the necessity of transmitting the generated key from the network center/base station to the wireless terminals, which is beneficial because Mizikovsky discloses that it is unwise to transmit a secret key over a wireless channel (Col. 1, lines 65-66). Therefore, improving the key distribution protocol of Tatebayashi with the teachings of Mizikovsky would have been obvious to one of ordinary skill in the art at the time the invention was made in order to enhance the security of wireless communication infrastructure as taught in Mizikovsky (Col. 8, lines 14-19) by not having the secret keys transmitted over the air.

Applicant's argument that the prior art does not disclose the first partial key value being sent to the second node after being decrypted by the super node such that the second node can use, in part, the decrypted first partial key in establishing the cryptographic key is not persuasive because Mizikovsky discloses a method of generating cryptographic keys for communication between a first node and a second node wherein the first and second nodes generate random seeds that are communicated through a base station to the other node. Once the random seed of the other node is received a common cryptographic key is generated and used for communication (Col. 7, lines 9-65. This meets the limitation because the random seed of the first station is sent to the second node to generate a common cryptographic key.

Applicant's arguments with respect to claim 4 are not persuasive because one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). .

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 1, 3, 5, 6, 7, 10, 11, 14-16, 19, 21, 23-25, 28, 29, 32-34, 37, 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tatebayashi, in view of Mizikovsky, U.S. Patent No. 5,748,734 as applied to claims 1, 4 above, and further in view of Menezes. Referring to claims 1, 3, 5, 6, 15, 16, 19, 21, 23, 24, 33, 34, 37, 38, Tatebayashi discloses a key distribution protocol wherein when a first user at a first terminal desires to share a common key or secret key with a second user at a second terminal, the first user generates a random number as a first key encryption key. The first key encryption key signal is passed to the network center using a public key scheme (Section 3), which meets the limitation of sending a first message from the first node to the super node, wherein the first message includes a first partial key value encrypted using a public key belonging to the super node, whereby encrypting with the public key requires less

energy than decrypting with a private key corresponding to the public key. The network center receives the key encryption key (Section 3), which meets the limitation of recovering the first partial key value at the super node by decrypting using the private key. Mizikovsky discloses a method of generating cryptographic keys for communication between a first node and a second node wherein the first and second nodes generate random seeds that are communicated through a base station to the other node. Once the random seed of the other node is received a common cryptographic key is generated and used for communication (Col. 7, lines 9-65), which meets the limitation of securely communicating the first partial key value to the second node, establishing the cryptographic key at the second node using the first partial key value and a second partial key value created by the second node, sending a third message from the second node to the super node, wherein the third message includes the second partial key value encrypted using the public key belonging to the super node, recovering the second partial key value at the super node by decrypting using the private key, securely communicating partial key value to the first node, and establishing the cryptographic key at the first node using the first partial key value and the second partial key value. Mizikovsky discloses that use of verification information that is transferred between the wireless terminals to authenticate the key transmissions (Col. 7, line 58 – Col. 8, line 14), but does not disclose that the verification information is a hash or a MAC. Menezes discloses that MACs are used for data verification (Page 362). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use MAC codes in the key distribution protocol of Tatebayashi in order to provide transaction authentication of exchanges between parties as taught in Menezes.

Referring to claims 7, 10, 11, 14, 25, 28, 29, 32, Mizikovsky discloses that central facility or network center stores the private keys for all users in a classic key system (Section 2.1), which meets the limitation of encrypting communications from the super node to a selected node using the symmetric key of that selected node.

4. Claims 8, 9, 12, 13, 17, 18, 26, 27, 30, 31, 35, 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tatebayashi, in view of Mizikovsky, U.S. Patent No. 5,748,734 as applied to claims 1, 4, 7, 11 above, and further in view of Menezes. Referring to claims 8, 12, 17, 18, 26, 30, 35, 36, Tatebayashi discloses a key distribution protocol wherein when a first user at a first terminal desires to share a common key or secret key with a second user at a second terminal, the first user generates a random number as a first key encryption key. The first key encryption key signal is passed to the network center using a public key scheme (Section 3), which meets the limitation of sending a first message from the first node to the super node, wherein the first message includes a first partial key value encrypted using a public key belonging to the super node, whereby encrypting with the public key requires less energy than decrypting with a private key corresponding to the public key. The network center receives the key encryption key (Section 3), which meets the limitation of recovering the first partial key value at the super node by decrypting using the private key. Mizikovsky discloses a method of generating cryptographic keys for communication between a first node and a second node wherein the first and second nodes generate random seeds that are communicated through a base station to the other node. Once the random seed of the other node is received a common cryptographic key is generated and used for communication (Col. 7, lines 9-65), which meets the limitation of securely communicating the first partial key value to the second node, establishing

the cryptographic key at the second node using the first partial key value and a second partial key value created by the second node, sending a third message from the second node to the super node, wherein the third message includes the second partial key value encrypted using the public key belonging to the super node, recovering the second partial key value at the super node by decrypting using the private key, securely communicating partial key value to the first node, and establishing the cryptographic key at the first node using the first partial key value and the second partial key value. Mizikovsky does not disclose the use of certificates to validate the keys used during the communication process. Menezes discloses methods of key distribution and key management wherein the symmetric keys used to set up secure communications are validated using certificates (Pages 554-555). It would have been obvious to one of ordinary skill in the art at the time the invention was made to validate the symmetric keys of Mizikovsky in order to avoid the requirement of either user terminal or node maintaining a secure database of user secrets as taught in Menezes (Page 554).

Referring to claims 9, 13, 27, 31, Menezes discloses that the certificates have a period of validity that would require the acquisition of new symmetric keys (Page 554), which meets the limitation of the certificate includes validation information for a plurality of symmetric keys and wherein a new second node symmetric key is selected periodically from the plurality of symmetric keys. It would have been obvious to one of ordinary skill in the art at the time the invention was made to validate the symmetric keys of Mizikovsky in order to avoid the requirement of either user terminal or node maintaining a secure database of user secrets as taught in Menezes (Page 554).

5. Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatebayashi, in view of Mizikovsky, U.S. Patent No. 5,748,734 and further in view of Menezes. Referring to claim 39, Tatebayashi discloses a key distribution protocol wherein when a first user at a first terminal desires to share a common key or secret key with a second user at a second terminal, the first user generates a random number as a first key encryption key. The first key encryption key signal is passed to the network center using a public key scheme (Section 3), which meets the limitation of sending a first message from the first node to the super node, wherein the first message includes a first partial key value encrypted using a public key belonging to the super node, whereby encrypting with the public key requires less energy than decrypting with a private key corresponding to the public key. The network center receives the key encryption key (Section 3), which meets the limitation of recovering the first partial key value at the super node by decrypting using the private key. Tatebayashi does not disclose that the network center transmits the key encryption key of the first node to the second node, the key encryption key of the second node to the first node, or establishing the common or secret key for communication between the first node and the second node by the first and second nodes using the received partial keys. Mizikovsky discloses a method of generating cryptographic keys for communication between a first node and a second node wherein the first and second nodes generate random seeds that are communicated through a base station to the other node. Once the random seed of the other node is received a common cryptographic key is generated and used for communication (Col. 7, lines 9-65), which meets the limitation of securely communicating the first partial key value to the second node, establishing the cryptographic key at the second node using the first partial key value and a second partial key value created by the second node,

sending a third message from the second node to the super node, wherein the third message includes the second partial key value encrypted using the public key belonging to the super node, recovering the second partial key value at the super node by decrypting using the private key, securely communicating partial key value to the first node, and establishing the cryptographic key at the first node using the first partial key value and the second partial key value. Mizikovsky discloses that central facility or network center stores the private keys for all users in a classic key system (Section 2.1), which meets the limitation of encrypting communications from the super node to a selected node using the symmetric key of that selected node, wherein the first and second node symmetric key is saved at the super node so that a subsequent key establishment can use symmetric key encryption for encrypting the first partial key value. It would have been obvious to one of ordinary skill in the art at the time the invention was made to the generate the common cryptographic key of Tatebayashi in the nodes as well as the network center in order to enhance the security of wireless communication infrastructure as taught in Mizikovsky (Col. 8, lines 14-19). Mizikovsky discloses that use of verification information that is transferred between the wireless terminals to authenticate the key transmissions (Col. 7, line 58 – Col. 8, line 14), but does not disclose that the verification information is a hash or a MAC. Menezes discloses that MACs are used for data verification (Page 362), which meets the limitation of a second message is sent from the first node to the second node, wherein the second message includes a first message authentication code, wherein the first partial key value is authenticated at the second node using the first message authentication code, wherein a fourth message is sent from the second node to the first node, wherein the fourth message includes a second message authentication code, wherein the second partial key value is authenticated at the

first node using the second message authentication code, establishing the cryptographic key at the first and second nodes by hashing the first and second partial key values. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use MAC codes in the key distribution protocol of Tatebayashi in order to provide transaction authentication of exchanges between parties as taught in Menezes. Mizikovsky does not disclose the use of certificates to validate the keys used during the communication process. Menezes discloses methods of key distribution and key management wherein the symmetric keys used to set up secure communications are validated using certificates (Pages 554-555), which meets the limitation of trust of the super node is established at the first node and the second node by validating a certificate provided by a recognized certificate authority and presented to the first node and second node by the super node. It would have been obvious to one of ordinary skill in the art at the time the invention was made to validate the symmetric keys of Mizikovsky in order to avoid the requirement of either user terminal or node maintaining a secure database of user secrets as taught in Menezes (Page 554). Menezes discloses that the certificates have a period of validity that would require the acquisition of new symmetric keys (Page 554), which meets the limitation of the certificate includes validation information for a plurality of symmetric keys and wherein a new second node symmetric key is selected periodically from the plurality of symmetric keys. It would have been obvious to one of ordinary skill in the art at the time the invention was made to validate the symmetric keys of Mizikovsky in order to avoid the requirement of either user terminal or node maintaining a secure database of user secrets as taught in Menezes (Page 554).

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier